Servidores Web de Altas Prestaciones (2016-2017)
Grado en Ingeniería Informática
Universidad de Granada

Trabajo Final - MITM

Pablo Parra Garófano

29 de mayo de 2017

Índice

1. Descripción general:

El ataque Man In The Middle [3], o en español Hombre en el Medio, consiste en introducirse en la comunicación entre dos equipos para que todo el tráfico pase por nosotros y poder así desencriptar sus datos y leer, insertar o modificar mensajes contra la voluntad de los afectados sin que estos tengan conocimiento de que esta pasando con sus datos en esos instantes. Ejemplo gráfico:

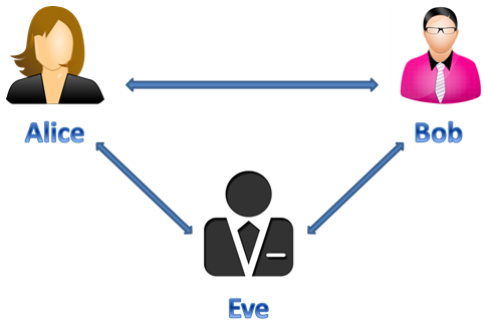

Figura 1.1: MITM común.

En el ejemplo de la imagen podemos ver un caso típico de man in the middle donde por ejemplo Alice envía su clave pública a Bob pero el mensaje es interceptado por Eve e Eve envía su clave a Bob y Bob queriendo enviársela a Alice la intercepta Eve e Eve le envía la suya a Alice. En el momento en que ellos cifren mensajes para enviarlos al otro Eve podrá leerlos ya que tiene las dos claves publicas de los dos atacados sin tener ninguno de ellos conocimiento de se encuentran charlando realmente con Eve. Eve podría modificar mensajes ya que se encuentra suplantando la identidad del otro, borrarlos o poner nuevos.

2. Subataques.

2.1. Interceptación de la comunicación.

Entraría el que hemos contado con anterioridad que es el más común y también incluiríamos el análisis del tráfico entre el usuario que se verá afectado y el servicio al que quiere acceder, accediendo en caso de no navegar por una red segura (HTTP) a los textos planos, ya que es muy complicado desencriptar los mensajes enviados por redes seguras.

2.2. Ataques de Sustitución (Spoofing).

El Spoofing en términos de seguridad hace referencia al uso generalmente malicioso de la suplantación de una identidad mediante el falseo de datos en una comunicación. Dependiendo de la tecnología utilizada podremos identificar diferentes tipos de spoofing, los más conocidos son:

- IP Spoofing
- ARP Spoofing

Donde IP Spoofing consiste en la modificar la dirección IP origen de un paquete TCP/IP por otra a la cual se desea suplantar. Y ARP Spoofing es la creación de tramas y falsificación de la tabla ARP donde tenemos la relación IP-MAC para que se envíen los datos/mesajes al atacante.

2.3. Ataques de reinyección:

Los ataques de repetición o REPLAY se suelen utilizar para capturar la información y posteriormente reenviarla con el objetivo de no solo de acceder a los datos, sino de tener la posibilidad de modificarlos y volver a insertarlos en la red.

2.4. Ataques de denegación de servicio (DoS).

Este tipo de ataques se utilizan para convertir el servicio o recurso que alguien ofrece en inaccesible a los usuarios. Normalmente se produce por el consumo del ancho de banda de la red de la victima o sobrecarga de los recursos del sistema atacado. Por ejemplo, el 27 de marzo de 2013 se produjo un ataque con correos basura de una empresa a otra provocando un funcionamiento lento de Internet en general.

3. Ataque real: Banco de Absa (África).

En 2013 se produjo un ataque a uno de los cuatro bancos más importantes de África (Absa) [1]. Fueron arrestadas 49 personas repartidas por toda Europa, los cuales fueron responsables de introducirse en la red del banco e introducir software malicioso. Y utilizando técnicas MITM, fueron capaces de captar correos y solicitudes de pago. Cuando vieron oportuno recrearon la página del banco (phishing) y enviaron correos falsos suplantando al banco para que se identificasen en su página recreada de forma que les estaban entregando usuarios y contraseña a los atacantes. Se transfirió a las cuentas de los atacantes la suma de 6.000.000 euros en escaso tiempo según informa la policía Europea. Seguidamente después de las transferencias sacaron el dinero fuera del alcance de la EU con una sofisticada red de transacciones de lavado de dinero.

4. ¿Por qué el uso de HTTPS?

HTTPS [4] viene a ser el uso normal de HTTP para que nuestro navegador se comunique con el servidor web pero funciona sobre SSL/TLS que son dos protocolos que convierten básicamente nuestra conexión insegura en segura. De forma que nos ofrecen:

- Encriptación: Aunque puedan interceptar nuestros mensajes no les será posible desencriptarlos.

- Integridad de los datos. Los mensajes que enviemos no pueden ser modificados.
- Autenticación. Gracias a los certificados de autoridad (CA), nos cercioramos de que estamos pidiendo un servicio a un servidor web que es quien dice ser.

5. Herramienta para MITM: Ettercap y Demo.

Ettercap [2] es un sniffer que nos permitirá una vez dentro de una red acceder a los diferentes mensajes que circulan entre los equipos que indiquemos que se encuentran dentro de dicha red.
Para instalarlo nos bastará con el comando:

```
sudo apt-get install ettercap-graphical
```

Así podremos trabajar con el de forma gráfica para esnifar dentro de una red. Cuando lo iniciemos deberemos de indicar la red de la que queremos esnifar:

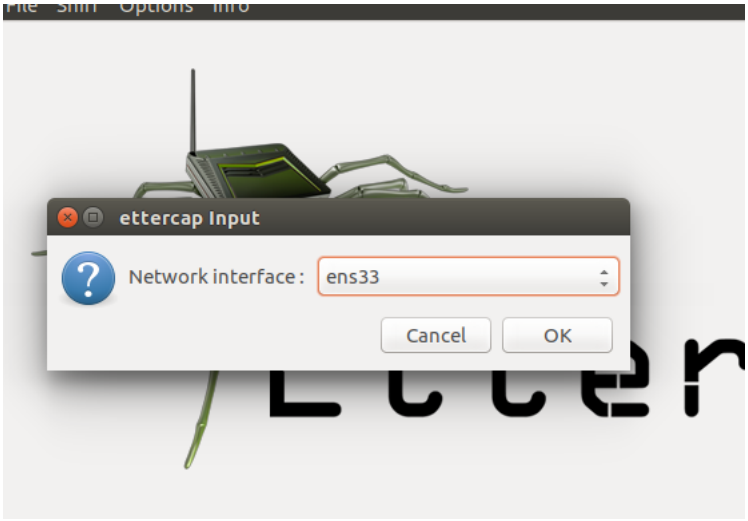

Figura 5.1: Red que queremos esnifar

Una vez seleccionada le diremos que escaneé los hosts que se encuentran en dicha red:

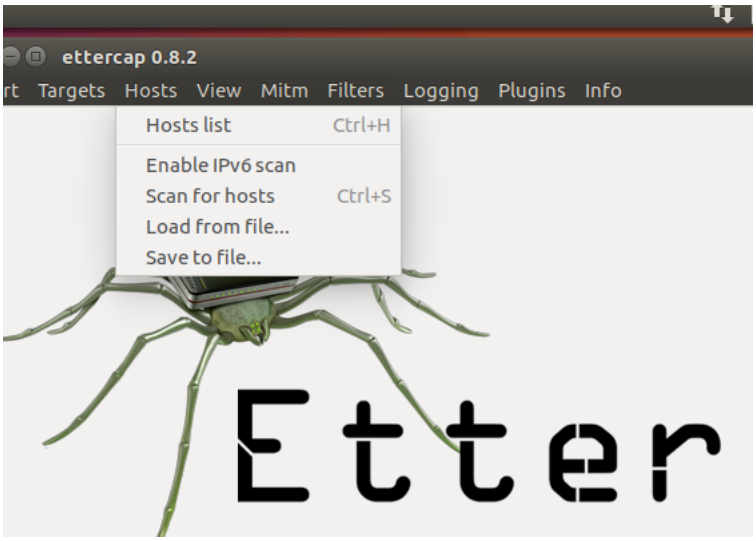

Figura 5.2: Scan for Hosts y Hosts List.

Los debemos añadir a los targets, es decir, podremos en diferentes target los hosts entre los que queremos esnifar. En mi caso serán por un lado la máquina afectada y por otro mi ordenador anfitrión que actúa de puente hasta internet:

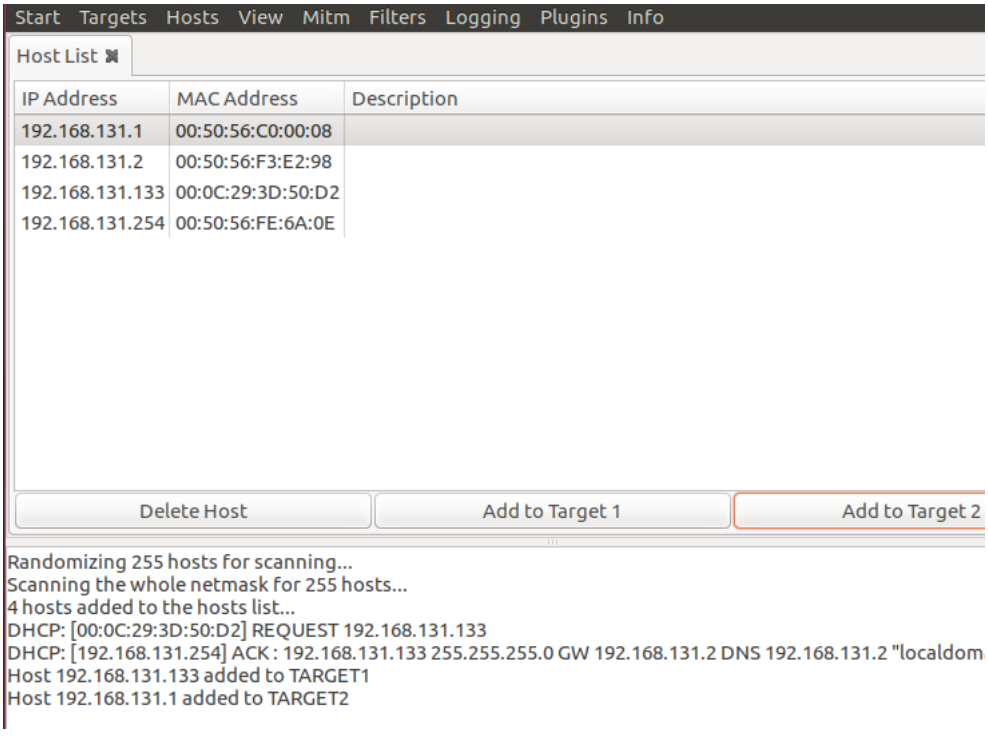

Figura 5.3: Añadir los equipos a los targets.

Desde la máquina atacante nos disponemos a realizar un ARP poisoning (En la aplica-

ción: Mimt->ARP Poisoning) y le damos a esnifar, desde la máquina afectada accedemos a servicio web que requiere login y que además no es segura, Podemos ver que nos aparece en texto plano tanto el usuario como la contraseña que enviamos. Ya podríamos acceder a este sitio suplantando a la persona en cuestión y obtener información sensible de forma que nuestro ataque hubiera funcionado con éxito.

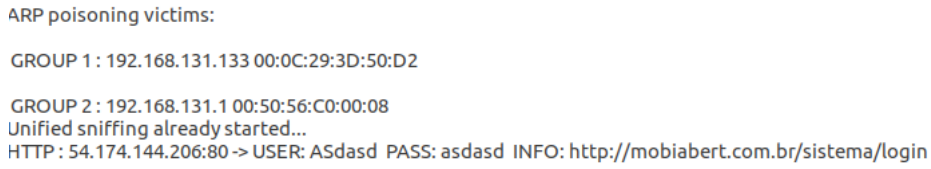

Figura 5.4: Usuario/Contraseña obtenida con éxito.

Referencias

[1] Articulo de robo con mitm. https://nakedsecurity.sophos.com/2013/04/19/anatomy-of-a-phish-how-to-spot-a-man-in-the-middle/.

[2] Instalar ettercap. http://curiosidadesvarias.portalfree.net/manual-de-como-instalar-ettercap-grafico-en-linux-ubuntu-kubuntu/.

[3] Man in the middle. http://www.cursodehackers.com/ManInTheMiddle.html.

[4] Porque usar https. https://www.arturogoga.com/especiales-que-es-https-y-por-que-y-como-debemos-activarlo/.